CLAIMS
(showing additions and deletions)

1. (Amended) A system for use by a customer to conduct a commercial transaction, the customer being registered and linked with an account for payment, the system comprising:

a. a host computer having access to data that links the customer with the customer account;

b. a first electronic device disposed at a point-of-sale terminal, the first electronic device being digitally linked to the host computer;

c. a second electronic device that is wireless, the wireless device being carried by the customer, the second electronic device communicating with the first electronic device transmitting data therebetween relative to an identity verification, radio frequency transmission being used for data transfer between the first electronic device and the second electronic device; and

d. a stylus having at least one sensor, the sensor capturing a digital signature of the customer while the stylus is being used;

wherein access to the customer account is enabled when the sensed digital signature matches a reference digital signature.

2. (Amended) The [identity authentication device] system of Claim 1, wherein the digital signature is a fingerprint.

3. (Amended) The [identity authentication device] system of Claim 1, wherein the digital signature involves the capture of cells from the customer touching the sensor.

4. (Amended) The [identity authentication device] system of Claim 1, wherein the

reference digital signature is disposed in the wireless device.

5. (Amended) The [identity authentication device] system of Claim 1, wherein the reference digital signature is disposed in a customer record, the customer record being accessible by the host computer.

6. (Amended) The [identity authentication device] system of Claim 1, wherein matching of the sensed print with the reference print occurs off-site.

7. (Amended) The [identity authentication device] system of Claim 1, wherein matching of the sensed print with the reference print occurs at a point-of-sale terminal.

8. (Amended) A system for use in regulating access to a secure area, the system including at least one pre-registered party who is permitted access to the secure area, the pre-registered party having previously submitted a reference digital signature, the system comprising:

a. a host computer that has access to data that links the registered party with the reference digital signature;

b. a first and a second electronic device, the first electronic device being disposed at a security check-point, the second electronic device being wireless, the second electronic device being carried by the customer, the first and second electronic devices being in communication with the host computer, radio frequency transmission being used for data transfer between the first electronic device and the second electronic device; and

c. a stylus having at least one sensor, the stylus being useful in preserving a log

of access to the secure area, the sensor capturing a digital signature of a party during engagement of a finger of the party with the stylus;

wherein access to the secure area is enabled when the sensed digital signature matches the reference digital signature.

9. (Amended) The [identity authentication device] system of Claim 8, wherein the digital signature is a fingerprint.

10. (Amended) The [identity authentication device] system of Claim 8, wherein the digital signature involves the capture of cells from the customer touching the sensor.

11. (Amended) The [identity authentication device] system of Claim 8, wherein the reference digital signature is disposed in memory within the wireless device.

12. (Amended) The [identity authentication device] system of Claim 8, wherein the reference digital signature is disposed in a customer record, the customer record being accessible through the host computer.

13. (Amended) The [identity authentication device] system of Claim 8, wherein comparison of the sensed print with the reference print occurs at a point-of-sale terminal.

14. (Amended) The [identity authentication device] system of Claim 8, wherein comparison of the sensed print with the reference print occurs at the security checkpoint.

15. (Amended) A method of conducting a commercial transaction for payment at a point-of-sale terminal, the method comprising:

d. requesting identity verification through cooperative engagement between a first and a second electronic device, the first electronic device being disposed at the point-of-sale terminal, the second electronic device being wireless, the second electronic device being carried by the customer, the first and second electronic devices being in digital communication with a host computer, the host computer having access to data that links at least one registered party to a reference digital signature;

e. using a stylus to submit written data pertinent to the identity verification, the stylus having a sensor that enables capture of a digital signature of a party during engagement of a finger of the party with the stylus;

f. transmitting data between the first electronic device and the second electronic device by radio frequency transmission; and

d. enabling access to the customer account when the sensed digital signature matches the reference digital signature.

16. (Amended) The [identity authentication device] method of Claim 15, wherein the digital signature is a fingerprint.

17. (Amended) The [identity authentication device] method of Claim 15, wherein the reference digital signature is disposed in the wireless electronic device.

18. (Amended) The [identity authentication device] method of Claim 15, wherein the reference digital signature is disposed in a customer record, the customer record being accessible by the host computer.

19. (Amended) The [identity authentication device] method of Claim 15, wherein matching of the sensed print with the reference print occurs at a point-of-sale terminal.

20. (Amended) The [identity authentication device] method of Claim 15, wherein matching of the sensed print with the reference print occurs at a point-of-sale terminal.

21. (Original) A method of enabling access to a secure area, the method comprising:

a. requesting identity verification through cooperative engagement between a first and a second electronic device, the first electronic device being disposed at a security checkpoint, the second electronic device being wireless, the second electronic device being carried by the customer, the first and second electronic devices being in digital communication with a host computer, the host computer having access to data that links at least one registered party to a reference digital signature;
b. using a stylus to submit written data pertinent to the identity verification, the stylus having a sensor that enables capture of a digital signature of a party during engagement of a finger of the party with the stylus;
c. transmitting data between the first electronic device and the second electronic device by radio frequency transmission; and
d. enabling access to the secure area when the sensed digital signature matches the reference digital signature.

22. (Amended) The [identity authentication device] method of Claim 21, wherein the

digital signature is a fingerprint.

23. (Amended) The [identity authentication device] method of Claim 21, wherein the reference digital signature is disposed in the wireless device.

24. (Amended) The [identity authentication device] method of Claim 21, wherein the reference digital signature is disposed in a customer record, the customer record being accessible by the host computer.

25. (Amended) The [identity authentication device] method of Claim 21, wherein comparison of the sensed print with the reference print occurs at the security checkpoint.

26. (Amended) A system for use by a customer to conduct a commercial transaction, the customer being registered and linked with an account for payment, the system comprising:

a. a host computer having access to data that links the customer with the customer account;
b. an electronic device disposed at a point-of-sale terminal, the electronic device being digitally linked to the host computer; and
c. a stylus that is wireless, the stylus being carried by the customer, a stylus having at least one sensor, the sensor capturing a digital signature of the customer while the stylus is being used, the stylus communicating with the electronic device transmitting data therebetween relative to an identity verification, at least some of the data transmission between the first electronic device to the second electronic device being by radio frequency;

wherein access to the customer account is enabled when the sensed digital signature matches a reference digital signature.

27. (Amended) The [identity authentication device] system of Claim 26, wherein the digital signature is a fingerprint.

28. (Amended) The [identity authentication device] system of Claim 26, wherein the digital signature involves the capture of cells from the customer touching the sensor.

29. (Amended) The [identity authentication device] system of Claim 26, wherein the reference digital signature is disposed in the wireless device.

30. (Amended) The [identity authentication device] system of Claim 26, wherein reference digital signature is disposed in a customer record, the customer record being accessible by the host computer.

31. (Amended) The [identity authentication device] system of Claim 26, wherein matching of the sensed print with the reference print occurs at a point-of-sale terminal.

32. (Amended) The [identity authentication device] system of Claim 26, wherein matching of the sensed print with the reference print occurs at a point-of-sale terminal.

33. (New) A system for use by a customer to conduct a commercial transaction, the customer being registered and digitally linked with an account for payment, the

system comprising:

e. a host computer having access to data that links the customer with the customer account;

f. a first electronic device disposed at a point-of-sale terminal, the first electronic device being digitally linked to the host computer;

g. a second electronic device that is wireless, the wireless device being carried by the customer, the second electronic device communicating with the first electronic device transmitting data therebetween relative to an identity verification, radio frequency transmission being used for data transfer between the first electronic device and the second electronic device; and

h. a stylus having at least one fingerprint sensor thereon, the sensor being capable of capturing a digital signature of the customer while the stylus is being used;

wherein the stylus is graspable between a thumb and one or more fingers of the customer's hand with an identifying portion of a thumb or finger of the customer contacting said fingerprint sensor, and wherein the stylus has a tip portion configured for marking on a paper or digital surface; and

wherein access to the customer account is enabled when the sensed digital signature matches a reference digital signature.